EU

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　２月２５日

出願番号
Application Number: 特願２０００－０４９９５０

出願人
Applicant (s): 株式会社エヌ・ティ・ティ・ドコモ

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年　７月２１日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０５７５１３

【書類名】　特許願
【整理番号】　DCMH110357
【提出日】　平成12年 2月25日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/14
【発明の名称】　ＰＣカード
【請求項の数】　6
【発明者】
【住所又は居所】　東京都港区虎ノ門二丁目１０番１号　エヌ・ティ・ティ移動通信網株式会社内
【氏名】　福本　雅朗
【発明者】
【住所又は居所】　東京都港区虎ノ門二丁目１０番１号　エヌ・ティ・ティ移動通信網株式会社内
【氏名】　杉村　利明
【特許出願人】
【識別番号】　392026693
【住所又は居所】　東京都港区虎ノ門二丁目１０番１号
【氏名又は名称】　エヌ・ティ・ティ移動通信網株式会社
【代理人】
【識別番号】　100098084
【弁理士】
【氏名又は名称】　川△崎▽　研二
【選任した代理人】
【識別番号】　100111763
【弁理士】
【氏名又は名称】　松本　隆
【選任した代理人】
【識別番号】　100108936

【弁理士】

【氏名又は名称】　秦　貴清

【手数料の表示】

【予納台帳番号】　038265

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ＰＣカード

【特許請求の範囲】

【請求項１】　外部機器に着脱されるＰＣカードであって、

コネクタを有する筐体部と、

該筐体部の表面に設けられ、使用者が把持する把持部と、

該把持部を使用者が把持したとき、使用者の生体情報を検出する生体情報検出手段と、

前記生体情報検出手段で検出された生体情報に基づいて特定の使用者か否かの本人認証を行う認証処理手段と、

前記生体情報検出手段及び認証処理手段を駆動するための電力を供給する内蔵電源と、を備えた

ことを特徴とするＰＣカード。

【請求項２】　前記筐体部が外部機器に装着されるとき、前記認証処理手段の認証結果に基づいて、当該ＰＣカードを外部機器に対して動作許可状態又は動作禁止状態にする

ことを特徴とする請求項１に記載のＰＣカード。

【請求項３】　前記生体情報検出手段は、前記把持部に設けられ、該把持部を把持する使用者の指紋情報を検出する

ことを特徴とする請求項１または２に記載のＰＣカード。

【請求項４】　請求項１または２に記載のＰＣカードにおいて、

前記認証処理手段による本人認証が完了してから所定時間の間、認証結果を出力する

ことを特徴とするＰＣカード

【請求項５】　請求項１～４に記載のＰＣカードにおいて、

当該ＰＣカードは、記憶媒体を備えた記憶装置である

ことを特徴するＰＣカード。

【請求項６】　請求項１～４に記載のＰＣカードにおいて、

当該ＰＣカードは、通信機能を前記外部機器に付加する通信装置である

ことを特徴とするＰＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、外部機器に着脱されるＰＣカードに係り、特に使用者の認証を行なうことのできるＰＣカードに関する。

【０００２】

【従来の技術】

近時、ポータブルＰＣ（パーソナルコンピュータ）等が普及し、その拡張デバイスとしてＰＣカード等のカード型拡張デバイスが多用されている。これらの拡張デバイスはポータブルＰＣ等に様々な機能を提供するものであり、例えば、半導体メモリやハードディスク等に情報を記憶するメモリデバイスとして機能するＰＣカードや、通信装置として機能するＰＣカード等が市販されている。

【０００３】

メモリデバイスの記憶容量は飛躍的に増大しており、メモリデバイスとして機能するＰＣカード内に秘密保持を要する情報が格納される可能性が高くなってきている。また、通信装置として機能するＰＣカードを用いてネットワークに接続し、ポータブルＰＣ等にて電子商取引や銀行取引の処理等を行ったりすることが多くなっている。即ち、ポータブルＰＣ等において秘密保持を要する情報が増え、これらの情報がメモリデバイスに内包したＰＣカード内に格納されることが多くなっている。

【０００４】

ところで、ＰＣカード等のカード型拡張デバイスは、ポータブルＰＣ等に対して着脱が容易であり、かつ単体での携行に好適であるため、紛失や、第三者による誤用等の発生を完全に排除することは困難である。即ち、カード型拡張デバイスに格納された秘密保持を要する情報が、第三者に利用される可能性がある。このような事態を回避するために、カード型拡張デバイスがポータブルＰＣ等の外部機器に装着された後に認証処理を行って、使用者が本人であるか否かの認証（以下、本人認証という）を行なうことが考えられる。

【０００５】

一般に、カードの使用者が本人であるか否かの認証を行う方法としては、磁気ストライプを有するカード（例えば、キャッシュカード）等においては磁気ストライプを読み取って当該カードに対応した暗証番号の入力を要求する方法や、認証データを記憶したＩＣカード等においてはその認証データを読み取って鍵情報を作成し、認証を行う方法等が広く知られている。また、より高度なセキュリティの確保やクレジットカード等を用いたキャッシュレスサービス等の実現を目的とし、使用者の生体情報（例えば、指紋、音声等）を用いた本人認証を行う方法も提案されている。

【０００６】

【発明が解決しようとする課題】

しかしながら、従来のＰＣカードやその他のカードを用いる本人認証は、カードを外部機器に装着した後に、この外部機器内の処理装置によって本人認証処理を行わせるため、カードを装着してから認証完了までに時間が必要となり、迅速な認証処理を実現することができなかった。

【０００７】

特に、外部機器（ＰＣカード等）のカードスロットにＰＣカードを指し込んで行う認証処理は、①ポータブルＰＣを起動し、ＰＣカードが装着されたか否かの認識、②本人認証に用いる使用者の情報および基準情報の読み込み、③使用者の情報と基準情報との比較照合、といった手順となる。このような、認証方法では、認証処理を外部機器に担わせているため、手間の掛かった操作性の悪いものとなっていた。

【０００８】

本発明は、以上の事情に鑑みてなされたもので、本発明は、ＰＣカードの使用に際し、使用者がＰＣカードを把持した段階で、本人認証を行うことができるＰＣカードを提供することを目的とする。

【０００９】

【課題を解決するための手段】

上記課題を解決するため、請求項１記載の発明は、外部機器に着脱されるＰＣ

カードであって、

コネクタを有する筐体部と、

該筐体部の表面に設けられ、使用者が把持する把持部と、

該把持部を使用者が把持したとき、使用者の生体情報を検出する生体情報検出手段と、

前記生体情報検出手段で検出された生体情報に基づいて特定の使用者か否かの本人認証を行う認証処理手段と、

前記生体情報検出手段及び認証処理手段を駆動するための電力を供給する内蔵電源と、を備えた

ことを特徴としている。

【００１０】

請求項２記載の発明は、前記筐体部が外部機器に装着されるとき、前記認証処理手段の認証結果に基づいて、当該ＰＣカードを外部機器に対して動作許可状態又は動作禁止状態にする

ことを特徴としている。

【００１１】

請求項３記載の発明は、前記生体情報検出手段は、前記把持部に設けられ、該把持部を把持する使用者の指紋情報を検出する

ことを特徴としている。

【００１２】

請求項４記載の発明は、請求項１または２に記載のＰＣカードにおいて、

前記認証処理手段による

本人認証が完了してから所定時間の間、認証結果を出力する

ことを特徴としている。

【００１３】

請求項５記載の発明は、請求項１～４に記載のＰＣカードにおいて、

当該ＰＣカードは、記憶媒体を備えた記憶装置である

ことを特徴としている。

【００１４】

請求項６記載の発明は、請求項１～４に記載のＰＣカードにおいて、
当該ＰＣカードは、通信機能を前記外部機器に付加する通信装置である
ことを特徴としている。

【００１５】

【発明の実施の形態】

以下、本発明の好ましい実施形態について図面を参照しつつ説明する。

【００１６】

（１）実施形態

（１－１）ＰＣカードの構成

図１ないし図３は、本発明に係るＰＣカードの一実施形態を示す図あり、本実施形態では、ＰＣカードスタンダード形のものを例示する。

【００１７】

まず、図１の概略構成図に基づいてＰＣカード１の構成について説明する。

ＰＣカード１は、所定記憶容量の記憶媒体を有するメモリデバイスとして機能するものである。なお、本発明によるＰＣカード１は、メモリデバイスに限定される趣旨ではなく、通信装置として機能するもの、或いは他の拡張デバイスであってもよい。

このＰＣカード１は、把持部２ａを有する筐体部２と、生体情報検出手段（ＳＣＮ）３と、マイクロコントローラ（ＭＣ）４と、メモリ（ＭＥＭ）５と、バッテリー（ＢＴ）６と、コネクタ７とによって大略構成されている。そして、ＰＣカード１は、図２に示すように、筐体部２がそのタイプに対応する所定形式のＰＣカードスロット９ａを持つポータブルＰＣ等の外部機器９に装着されるようになっている。

【００１８】

ここで、筐体部２は、ＰＣカード１の外形をなし、この筐体部２には使用者がＰＣカード１を持ち易くする把持部２ａが形成されている。また、把持部２ａには、この把持部２ａを把持する使用者の指紋情報を検出する生体情報検出手段３が装着されている。

この生体情報検出手段３は、筐体部２の少なくとも片面側の所定位置（両面の

異なる位置でもよい）で使用者の指紋情報を検出するものである。生体情報検出手段３は、カード把持時に把持部２ａに密着した指の指紋だけが読取可能なように、公知のＣＣＤ（Charge Coupled Device：電荷結合素子）等によって構成されている。

また、生態情報検出手段３は、使用者の指紋を検出するのみでなく、使用者の把持状態を検知するスイッチを把持部２ａに備え、使用者が把持部２ａを把持したときに、マイクロホンで使用者の音声を読込み、この音声を分析して生体情報として検出してもよい。なお、スイッチは機械的なスイッチに限らず、例えば、把持部２ａに圧力センサを設け、使用者のカード１を把持する圧力によってスイッチング動作を行ったり、筐体部２の先端に接触センサを設け、カードスロット側のシャッタを開いたときにスイッチング動作を行うようにして、スイッチの代用とすることも可能である。

【００１９】

マイクロコントローラ４及びメモリ５は、指紋情報に基づいて使用者が特定の使用者か否かの本人認証を行う認証処理を行うものである。このマイクロコントローラ４は、生体情報検出手段３で検出された指紋データからその指紋の特徴パターンを抽出する処理を実行する。また、マイクロコントローラ４は、後述する認証処理プログラムに従ってこの特徴パターンに基づいて認証を行う。

また、メモリ５の所定領域には、認識処理を実行するための制御プログラムと、予め記憶した登録データ（特定の使用者の指紋の特徴パターンデータ等）が記憶されている。

【００２０】

具体的には、マイクロコントローラ４は、メモリ５に格納された制御プログラムに従って、予め記憶した登録データ（特定の使用者の指紋の特徴パターンデータ）をメモリ５の所定領域から読み出し、生体情報検出手段３で読み取った指紋情報について特徴抽出処理を行なった結果の指紋のパターンデータと比較照合する。この場合、読み取り範囲と登録パターンの範囲との関係は、例えば読み取り範囲を広く、登録パターンの範囲を狭くする。これにより、マイクロコントローラ４による比較照合は、読み取り範囲をサーチ領域とし、このサーチ領域内で指

紋の登録パターンと類似のものを指紋の長さや間隔、形状等からサーチする、といった比較を行う。

【００２１】

その照合の結果、双方の指紋の特徴パターンが一致すると判定されれば本人である旨の認証結果に対応した信号をコネクタ７から出力し、認証完了後にＰＣカード１を所定の動作許可状態にする。この状態で、ＰＣカード１が外部機器９等に装着された場合には、このＰＣカード１は動作可能となる。

一方、照合の結果、双方の指紋の特徴パターンが一致しなければ、本人でない旨の認証結果に対応した信号をコネクタ７から出力し、認証前の状態と同様の所定の動作禁止状態となる。この動作禁止状態では、ＰＣカード１が外部機器９に接続されても外部機器９に全く応答せずに動作させないか、若しくは、その機能の一部に制限が加えられた状態となる（例えば、通信装置の発信動作や、ファイルシステム内の特定のファイルやディレクトリへのアクセスができなくなる等の状態となる）。

ここにいう動作禁止状態とは、外部機器９等からＰＣカード１に対してアクセスができない状態である。また、外部機器９に動作禁止状態にあるＰＣカード１が装着された場合であっても、ＰＣカード１の把持部２ａを使用者が把持して生体情報が入力されたときには、即座にその生体情報（指紋情報）を読み取って前記認証処理を行うことも可能である。

なお、指紋データの比較照合の方法は、例えば特開平１０－３１２４５９号公報等に開示されている。

【００２２】

また、マイクロコントローラ４の内部には図示しないタイマ機構を有しており、使用者の把持による認証完了後に、一定の所定時間内に外部機器９への挿入（正常な接続状態となる装着）がなされない場合には、既に行なった認証結果を無効とすることにより、情報に対するセイキュリティ性能を向上させるようにしている。

【００２３】

さらに、マイクロコントローラ４は、使用者がカードの所有者等である認証が

完了した場合、所定の方式で暗号化した所定のユーザ識別コードやパスワード情報等をコネクタ７を介して外部機器９側に出力し、外部機器９側で使用者を認証させることも可能である。

【００２４】

コネクタ７は、筐体２の先端側（図２中の右側）に設けられたものであり、このコネクタ７は、例えばＰＣカード・スタンダード（ＰＣ Card Standard）形式に対応したものである。

なお、コネクタ７は、これに限らず、携帯端末その他の外部情報機器との接続用のコネクタを構成できる汎用性の高い他形式のもの、例えばコンパクトフラッシュ・タイプII（Compact Flash Type II）に対応したものでもよい。

ここで、ＰＣカード・スタンダードとは、ＪＥＩＤＡ（Japan Electronics Industry Development Association：日本電子工業振興協会）と米国ＰＣＭＣＩＡ（Personal Computer Memory Card International Association）が共同で制定したＰＣカードの規格であり、厚さによって異なるタイプI、タイプII、タイプIII、タイプIV等がある。コンパクトフラッシュ（Compact Flash）・タイプは更に小型で、タイプIIは縦横が42.8 ×36.4、厚さが5.0(mm)である。このため、これらに対応したコネクタをコネクタ７に採用した場合には、ＰＣカード１の小型化が容易となる。

【００２５】

（１－２）認証処理の動作

次に、ＰＣカード１による認証処理の動作について、図３のフローチャートを参照しつつ説明する。

【００２６】

上述のように構成された本実施形態においては、使用者がＰＣカード１の筐体部２の把持部２ａを把持すると、バッテリー６の電力がマイクロコントローラ４、生体情報検出手段３等に供給され、これらを駆動して認証処理が開始される。マイクロコントローラ４は、生体情報検出手段３によって使用者の指紋情報の読み取りを行う（ステップＳ１）。

【００２７】

次いで、マイクロコントローラ４は、生体情報が入力されたか否か、即ちＰＣカード１の筐体部２の把持部２ａに密着した使用者の指紋が入力されたか否かをチェックし（ステップＳ２）、指紋情報が入力されていれば（ステップＳ２；ＹＥＳ）、その指紋データに基づいてその指紋の特徴の抽出処理が実行される（ステップＳ３）。また、これと同時に、或いはこれに先立って、マイクロコントローラ４は、登録された使用者の指紋の特徴データをメモリ５から読み出す（ステップＳ４）。

一方、マイクロコントローラ４は、指紋情報が入力されない場合（ステップＳ２；ＮＯ）には、使用者がカード把持してから所定時間が経過したか否かがチェックされ（ステップＳ１１）、所定時間が経過していなければ、再度、指紋情報の入力とそのチェックがなされる（ステップＳ１，Ｓ２）。

〔００２８〕

次いで、マイクロコントローラ４は、今回入力された指紋の特徴と登録された使用者の指紋の特徴とが一致するかを比較照合し（ステップＳ５）、双方の特徴が一致するか否かが判定される（ステップＳ６）。

〔００２９〕

そして、マイクロコントローラ４は、その処理結果に応じて、双方の指紋の特徴が一致する場合（ステップＳ６；ＹＥＳ）には、カード装着後にＰＣカード１の動作が可能な所定の動作許可状態とし（ステップＳ７）、双方の指紋の特徴が一致しない（ステップＳ６；ＮＯ）場合には、カード装着後にＰＣカード１の動作ができない動作禁止状態にする（ステップＳ１０）。

なお、動作禁止状態において、未認証により動作禁止状態である旨の信号を外部機器９側に向けて報知する信号出力を行なうようにしてもよい。

〔００３０〕

また、ステップＳ７で動作許可状態になると、マイクロコントローラ４は、その後の所定時間内にＰＣカード１が外部機器９のＰＣカードスロット９ａに挿入されて、正常に接続されたか否かをチェックする（ステップＳ８）。

所定時間内にＰＣカード１がＰＣカードスロット９ａに挿入された場合（ステップＳ８；ＹＥＳ）には、マイクロコントローラ４は、所定時間毎にＰＣカード

１が外部機器９のＰＣカードスロット９ａから外されたか否かをチェックする（ステップＳ９）。

一方、ＰＣカード１が外部機器９のＰＣカードスロット９ａに正常に挿入されないまま所定時間が経過した場合（ステップＳ８；ＮＯ）、または正常な挿入後にＰＣカード１が外された場合（ステップＳ９；ＹＥＳ）、マイクロコントローラ４は、その時点でＰＣカード１を動作禁止状態にする（ステップＳ１０）。

【００３１】

（１－３）実施形態の効果

このように本実施形態においては、使用者がＰＣカード１の把持部２ａを把持した段階で認証処理を行うため、外部機器９にＰＣカード１が装着するときには、本人の認証が確認でき、従来のようにＰＣカードを外部機器（例えば、ポータブルＰＣ）に装着した後に面倒な認証処理のためのパスワード入力等を行ったりする必要がなくなる。

即ち、本実施形態では、カード装着に先立ってＰＣカード１を使用者が把持することにより、迅速な本人認証を行うことができ、装着後に認証処理を行う必要がなくなる。

【００３２】

従って、ＰＣカード１は、メモリカードに限らず、他のストレージ系ＰＣカードであっても、このＰＣカード１内の記憶情報を保護するプロテクト機能を付加しながら、ＰＣカード１に対する情報の迅速な書き込み／読み出しが可能となる。

【００３３】

また、本実施形態においては、マイクロコントローラ４にタイマ機能を持たせて、認証後の一定時間内に正常な接続がなされないときは認証結果を無効にするようにしているので、ＰＣカード１のセキュリティ性能をより向上させることができる。

【００３４】

さらに、外部機器９にＰＣカード１が装着された後は、このＰＣカード１は外部機器９の一部として管理され、外部機器９の使用者の認証処理等に応じて使用

される。勿論、拡張デバイスとしてのＰＣカード１にパスワードを設定しておき、電源投入後の最初の使用時にパスワード入力を要求したり、カード外端面部（挿入方向後端）のＰＣカード1若しくは外部機器９側のマイクロホンで入力した音声の特徴を抽出することで再度認証を行なうことも可能である。

〔００３５〕

（２）変形例

（２－１）変形例１

変形例１によるＰＣカード１２は、生体情報検出手段をカード両面（表裏両面）の把持部１２ａと幅方向両側の側面１２ｂと後端面１２ｃとに、それぞれに配置された点にある。

ＰＣカード１２には、その起端側を覆うように、カード両面（表面及び裏面）の把持部１２ａと、両側の把持部１２ｂと、起端面の把持部１２ｃとによって形成されている。そして、これらの把持部のうち複数の箇所に、生体情報検出手段による指紋参照窓等が配置されている。

〔００３６〕

起端面の把持部１２ｃは、専ら挿入完了時に親指等で押圧される部分であり、カード把持時に単独で指に接し難いが、ＰＣカード１２の起端面以外の他の面と同時に把持され得るものであり、本発明にいう把持部に含まれる。各把持部１２ａ，１２ｂ，１２ｃにおける指紋参照窓等の形状や個数等が任意であることはいうまでもない。ＰＣカード１２の両面に形状の異なる指紋参照窓を設けたり、他種類の生体情報入力部（例えば音声入力部）を併設したりすることも可能である。

〔００３７〕

（２－２）変形例２

前記各実施形態では、ＰＣカード１をメモリデバイスとして用いた場合を例示したが、通信装置等のモデム機能を持つＰＣカードであっても、そのＩＤ格納メモリ、その他のメモリに使用者の指紋の特徴データを記憶させておき、マイクロコントローラ４による認証処理を行なうことも可能である。従って、ＰＣカード１が、通信機能を備えたＰＣカードであれば、このＰＣカード１による通信回線

の不正使用を防止しながら迅速な回線接続ができる。

【００３８】

【発明の効果】

本発明によれば、外部機器へのＰＣカードの装着に先立って、ＰＣカードを使用者が把持することにより、本人認証をＰＣカード自体で迅速に完了する。これにより、装着後の本人認証の処理を省略することができる。この結果、ＰＣカードがメモリデバイスとして機能するものであれば、このカード内の記憶情報を保護するプロテクト機能を付加しながら、迅速な書き込み／読み出しができ、ＰＣカードが通信装置として機能するものであれば、このカードによる通信回線の不正使用を防止しながら迅速な回線接続を可能とする。

【図面の簡単な説明】

【図１】　本発明の実施形態に係るＰＣカードの概略構成を示すブロック図である。

【図２】　同実施形態のＰＣカードの把持部周辺を示す上面図である。

【図３】　同実施形態に係るＰＣカードの認識処理手順を説明するフローチャートである。

【図４】　本発明の変形例に係るＰＣカードの把持部周辺の外観図で、（ａ）はその平面図、（ｂ）はその側面図である。

【符号の説明】

１、１２・・・ＰＣカード

２・・・筐体部

２ａ、１２ａ、１２ｂ・・・把持部

１２ｃ・・・後端面（把持部）

３・・・生体情報検出手段（指紋入力手段）

４・・・マイクロコントローラ（認証処理手段）

５・・・メモリ

６・・・バッテリー（内蔵電源）

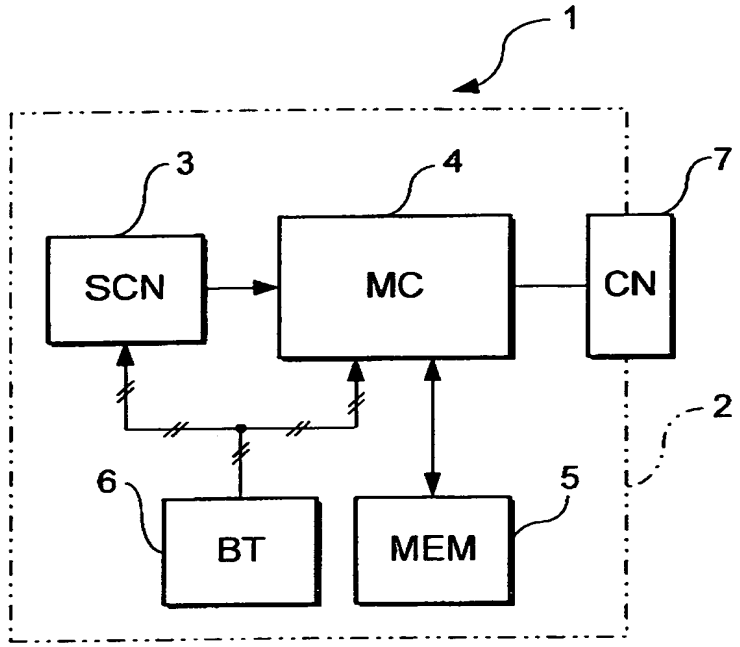
７・・・コネクタ

９・・・外部機器

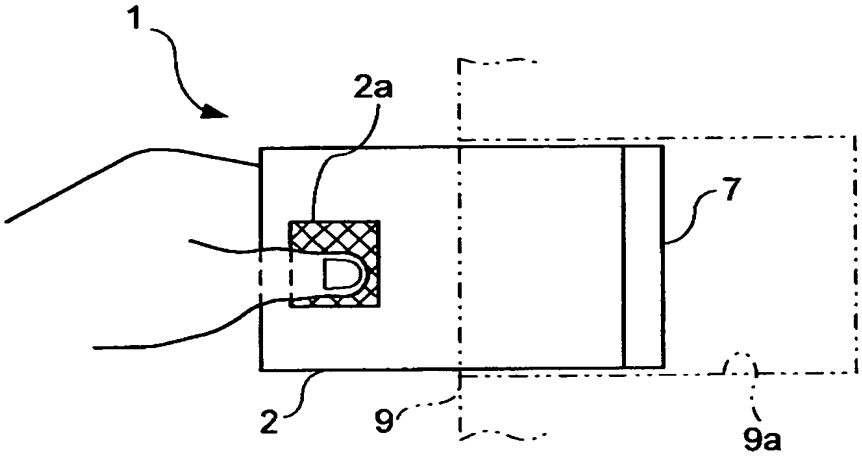
９ａ・・・ＰＣカードスロット

【書類名】　　図面

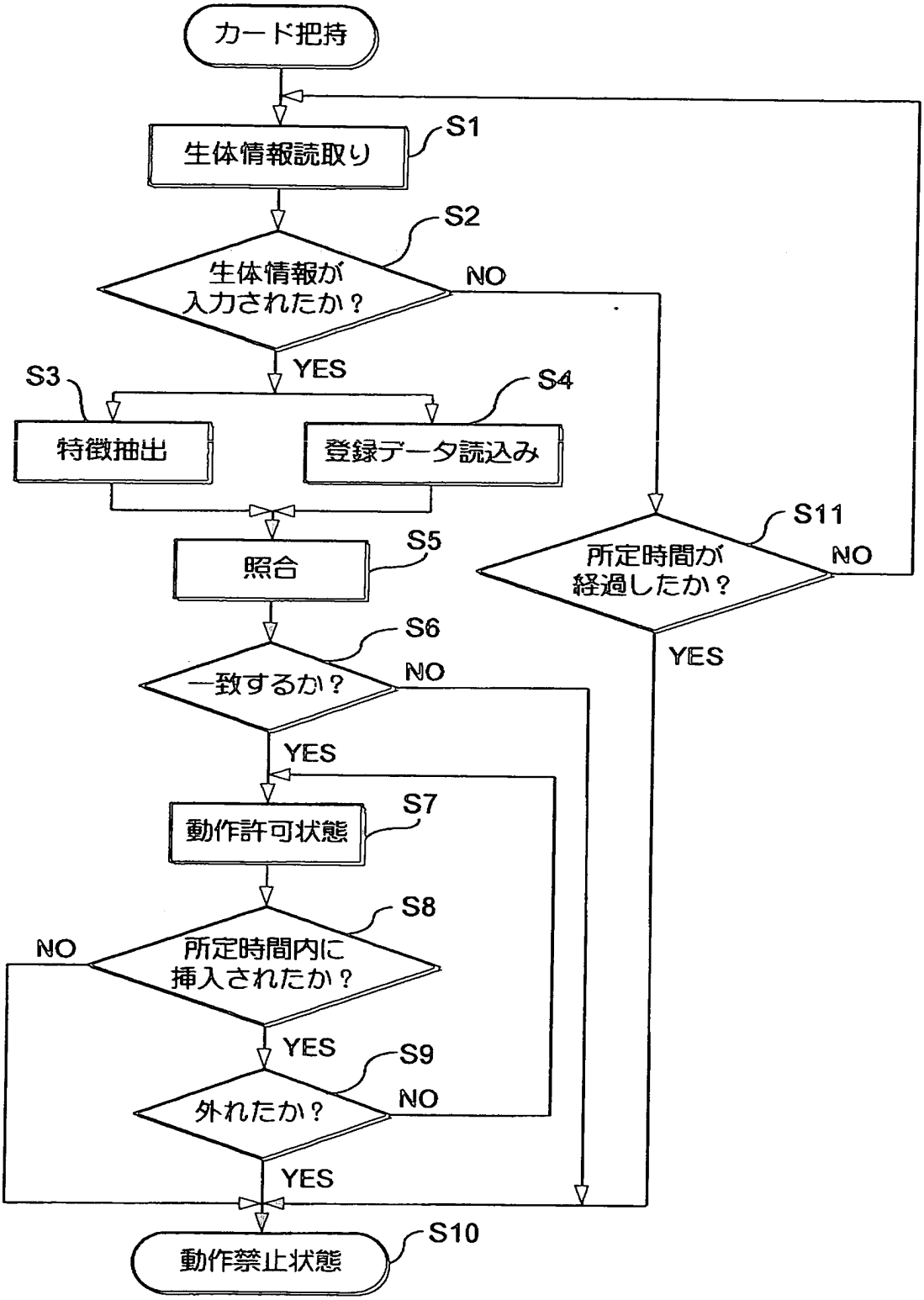
【図１】



【図２】

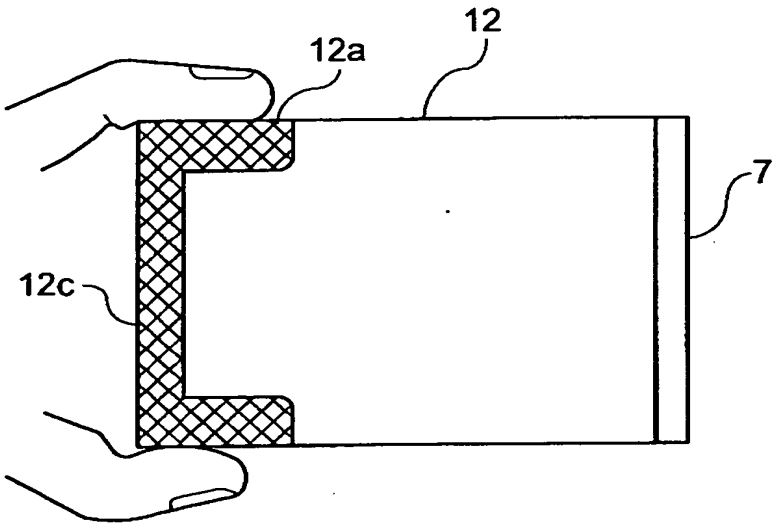


【図３】

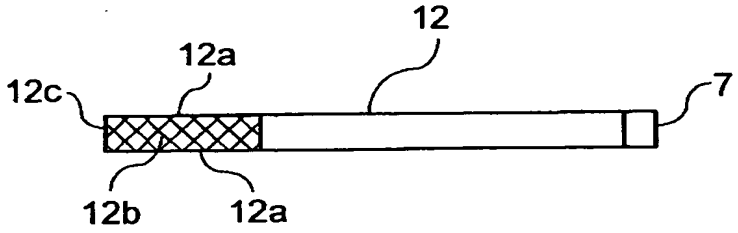

カード把持
生体情報読取り
S1
生体情報が
入力されたか？
S2
NO
YES
S3
特徴抽出
S4
登録データ読込み
照合
S5
一致するか？
S6
NO
YES
所定時間が
経過したか？
S11
NO
YES
動作許可状態
S7
所定時間内に
挿入されたか？
S8
NO
YES
外れたか？
S9
NO
YES
動作禁止状態
S10

【図４】

(a)



(b)



【書類名】　　要約書

【要約】

【課題】　外部機器へのカード装着に先立って、使用者がＰＣカードを把持することにより、本人認証を行う。

【解決手段】　ＰＣカード１の筐体部２には、筐体部２を外部機器に装着する際に使用者に把持される把持部が形成され、この把持部には使用者の指紋情報を入力するＳＣＮ９が設けられる。マイクロコントローラ４は、ＳＣＮ９からの指紋情報に基づいて特定の使用者か否かの認証処理を行う。ＰＣカード１を外部機器に装着する前に、認証処理の結果に基づいて、ＰＣカード１を所定の動作許可状態又は動作禁止状態にする。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔３９２０２６６９３〕

１．変更年月日　１９９２年　８月２１日
［変更理由］　新規登録
住　所　東京都港区虎ノ門二丁目１０番１号
氏　名　エヌ・ティ・ティ移動通信網株式会社

２．変更年月日　２０００年　５月１９日
［変更理由］　名称変更
住　所　東京都千代田区永田町二丁目１１番１号
氏　名　株式会社エヌ・ティ・ティ・ドコモ